UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/490,354	01/24/2000	Noriya Kobayashi	UCSD	7055

24978 7590 10/25/2004

GREER, BURNS & CRAIN
300 S WACKER DR
25TH FLOOR
CHICAGO, IL 60606

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/490,354	KOBAYASHI ET AL	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30,32-46 and 48-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30,32-46 and 48-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30, 32-46, 48-55 are pending. Claims 31 and 47 have been cancelled. Claims 2, 30, 34 and 45 have been amended.

2. The attorney's arguments have been considered and are addressed below.

3. With respect to Claim 34, the attorney's arguments are persuasive and hence the rejection has been adjusted and the new rejection can be found below. Due to this, this action has been made non-final.

Response to Arguments

1. The attorney argues that Rosen fails to teach calculating in the computer of the ticket provider by the use of a private key, s and a digital data D_3. This limitation is met by Rosen on column 7, lines 30-38. This reference discloses a digital signature and a private key being used to create a digital ticket. The merchant's advertisement/presentation of a potential ticket to be purchased represents D_1. (See Rosen on column 4, lines 33-39, 45-50, column 5, lines 59-67 and column 6, line 1). On column 5 and 6 of the cited reference, the ticket contains a preview of the content/ticket. The consumer cannot use the ticket until he pays for it (Rosen column 7, lines 2-8). The merchant's sending of electronic merchandise to the consumer on column 4, lines 33-39 relates to a preview/advertisement of the merchandise/ticket. This is because the consumer has to agree to purchase the ticket and complete the transaction before he can use the ticket (See Rosen, column 7, lines 56-61). Furthermore, the consumer's request for a ticket from a merchant constitutes D_2. This can be seen on Rosen column 4, lines 33-39. The unique ticket issued to the consumer by the merchant represents D_3.

2. *The attorney argues that Rosen fails to teach D_2 including a one-way function hash(R) of which R is uniquely known to the computer of the ticket consumer and not to the computer of the ticket provider.* Rosen on column 11, lines 31-67 and on Fig. 6A show the functions and makeup of a trusted server. X is equivalent to Cert(TS). Cert(TA) is a function of Cert(TS) and hence Cert(TS) is known to both the Computer Trusted Agent and the Merchant Trusted Agent. Therefore, because X is a function of a hash value it is a unique value to the merchant computer/ticket provider. Hence Rosen meets the given limitation.

3. *The attorney argues that Rosen does not appear to teach or suggest a method to permit purchasers to remain anonymous.* Please see Rosen, column 1, lines 65-67 and column 2, lines 1-8. Rosen clearly discloses consumer/user anonymity.

4. *With respect to Claim 8, the attorney argues that Rosen fails to teach or suggest at least calculating in the computer of a ticket consumer a number R, then second calculating in the computer of the ticket consumer a one-way function of the number R as hash(R) as defined.* X represents R and the h(X) represents the hash of X. The customer's trusted agent (CTA) represents an extension of the consumer terminal that allows ticket purchases and payment to be performed securely (Rosen, column 4, lines 6-10). Fig. 6A shows that X i.e. Cert(TS) is known to the computer of the ticket consumer since Cert(TA) is a function of Cert(TS) and is known to the Customer Trusted Agent (CTA).

5. *With respect to Claim 24, the attorney argues that Rosen fails to suggest a ticket provider's computer that digitally signs a ticket order data that is transmitted to the ticket consumer's computer.* This is disclosed by Rosen on column 7, lines 30-38. This limitation further illuminates the column 6, lines 7-12 quotation.

6. With respect to Claim 25 and 33, the attorney's argument has already been traversed in Claim 8 traversal.

7. With respect to Claim 30, the attorney's argument has already been traversed above.

8. With respect to Claim 34, the attorney's arguments are persuasive and hence its rejection has been adjusted and its new rejection can be found below.

9. *With respect to Claim 49 and 50, the attorney argues that Rosen fails to teach at least a ticket buyer computer sending at a first time a one-way transformation of a private number to a seller computer.* This has already been traversed above.

10. *With respect to Claim 38, the attorney argues that Mengin fails to teach at least a communication channel for at a second time, sending from a ticket buyer to a ticket seller data representative of a non-invertible transformation of a number determined by the ticket buyer only.* On paragraphs 51-53, the customer/ticket buyer generates a message

composed of self-identifying information. This message is called digamas and it is hashed. Hashing forms a non-invertible transformation of this message/number.

11. With respect to Claim 45, the attorney's arguments have already been traversed above.

12. With respect to Claim 51, the limitation argued by the attorney is not contained within Claim 51 limitation.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim1-5, 8, 12-15, 17, 22, 9-11, 24, 25, 29-30, 32-35, 49, 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosen (5557518).

With regards to Claim 1, the limitation of "first communicating, across a communications channel from a computer of a ticket provider to a computer of a prospective ticket consumer, first digital data D1 in respect of an occurrence for which tickets may be delivered; and then, the prospective ticket consumer deciding to obtain a digital ticket for the occurrence and thus to become a ticket consumer" is met on column 4, lines 33-39 and 45-50; and "second communicating, across the communications channel from the computer of the ticket consumer to the computer of the ticket provider,

second digital data D_2 including indication that a ticket is desired for the occurrence; and then, the ticket request being capable of being fulfilled" is met on column 4, lines 45-50; and "calculating in the computer of the ticket provider by use of a private key s a digital signature of third digital data D3, which third digital data D3 is in respect of one or both of the first digital data D1. and the second digital data D2, which digital signature of the digital data D3 is, as well being a proof both (i) that a private signature key s was Used by the computer of the ticket provider in generation of the digital signature and (ii) that one or both of the digital data D1, D2 was used in respect of its generation, (iii) suitably stored in a transportable storage medium" is met on column 7, lines 30-38 and on column 6, lines 7-8; and "wherein the digital data D1, D2 in respect of which the digital signature of digital data D3 was generated becomes a memorialization of a particular provision by the ticket provider of the particular digital ticket for the particular occurrence to the ticket consumer who is particularly identified at least as a party at the other end of the communicating transpiring across the communications channel" is met on column 7, lines 30-38 and column 6, lines 7-13; and "third communicating, across the communications channel from the computer of the ticket provider to the computer of the ticket consumer, at least the signed digital data D3" on column 7, lines 56-61; and "first storing with the computer of the ticket consumer in the transportable storage medium at least the signed digital data D3, thus turning the transportable storage medium into a digital ticket" on column 4, lines 41-51 and on column 9, lines 23-26; and "physically transporting the digital ticket in the form of the transportable storage medium so containing at least the signed digital data D3 to a specific time and place where the specific occurrence for which the digital ticket has been provided is to transpire" is met on column 25, lines 64-

67, column 26, lines 1-3 and on column 9, lines 63-66; and "tendering the digital ticket for redemption to a ticket taker at the specific occurrence; reading into a computer of the ticket taker at least the signed digital data D3" on column 24, lines 65-67, column 25, lines 1-5; and "recovering in the computer of the ticket taker, with a digital verification key v corresponding to the signature key s of the ticket provider and from the signed digital data D3, the digital data D3" on column 25, lines 7-15; and "determining in the computer of the ticket taker IF the digital data D3 was recoverable by verification key v AND, having been so recovered, the digital data D3 correctly memorializes the particular provision by the ticket provider of the particular third digital data D3 for the particular occurrence to the particular ticket consumer who at one time communicated across the communications channel THEN the digital ticket is valid, ELSE IF the digital data D3 was recovered by use of the verification key v BUT the digital data D3 recovered incorrectly memorializes the particular provision by the ticket provider of the particular third digital data D3, for the particular occurrence to the particular ticket consumer who at one time communicated across the communications channel THEN the digital ticket is invalid" on column 25, lines 14-23.

Rosen does not explicitly state the variables D1, D2 and D3, however Rosen defines various scenarios that meet the scenarios within the limitation that help define these variables and they are hereby discussed. The merchant's advertisement/presentation of a potential ticket to be purchased represents D_1. (See Rosen on column 4, lines 33-39, 45-50, column 5, lines 59-67 and column 6, line 1). On column 5 and 6 of the cited reference, the ticket contains a preview of the content/ticket. The consumer cannot use the ticket until he pays for it (Rosen column 7, lines 2-8). The

merchant's sending of electronic merchandise to the consumer on column 4, lines 33-39 relates to a preview/advertisement of the merchandise/ticket. This is because the consumer has to agree to purchase the ticket and complete the transaction before he can use the ticket (See Rosen, column 7, lines 56-61). Furthermore, the consumer's request for a ticket from a merchant constitutes D_2. This can be seen on Rosen column 4, lines 33-39. The unique ticket issued to the consumer by the merchant represents D_3.

It would have been obvious to one of ordinary skill in the art to have a ticket preview/advertisement represent D_1 because it is a digital data that is transmitted from the ticket provider to a prospective consumer and it allows the consumer to decide if he wants to buy the ticket or not.

With respect to Claim 2, the limitation "wherein the second communicating is of second digital data D2 including a one-way function **hash(R)** of a number R which number R is uniquely known to the computer of the ticket consumer and not to the computer of the ticket provider" is met on column 11, line 67; and "wherein the calculating in the computer of the ticket provider is of a digital signature in respect of the third digital data D, including the oneway function of **hash(R)** plus information I concerning the event for which theticket is had, wherein the third communicating is of **Sign (s, I hash (R)** wherein the first storing is of R appended to **Sign(s,I||hash(R)), or Sign(s,I||hash(R))||R,** as the digital ticket; wherein the reading into the computer of the ticket taker is of the **Sign(s,I||hash(R))||R.;** wherein the recovering in the computer of the ticket taker of the **I||hash (R)** gives **hash (R)** ; and, having both **R and hash (R)** to hand" is met on column 11, lines 14-67 and on column 12, lines 1-15.

Further limitation of "wherein the determining further proceeds by recalculating the **hash(R)** in respect of R, so that IF the recalculated **hash(R)** equals to the recovered **hash(R)** of the digital ticket as read THEN the digital ticket is valid ELSE. IF the **hash(R)** does not equal to the recovered **hash(R)** of the digital ticket as read THEN the digital ticket is invalid" is inherently met on column 12, lines 7-9.

With respect to Claim 3, the limitation of "wherein the determining still further proceeds so that IF the read digital ticket is the first uniquely presented THEN the digital ticket is valid ELSE IF the read. digital ticket is not the first uniquely presented THEN the digital ticket is invalid" is met on column 25, lines 15-18.

With respect to Claim 4, the limitation "wherein the second communicating is of a one-way hash function **hash(R)** of a number R" is met on column 12, lines 8-9; and "wherein the calculating in the computer of the ticket provider is of a digital signature in respect of signature key s of both the **hash(R)** plus information I concerning the event for which the ticket is had, **Sign(s,I||hash(R))"** is met on column 11, lines 14-67; and "wherein the third communicating is of **Sign(s,I||hash(R));** and wherein the first storing is of R appended to **Sign(s,I||hash(R)), or Sign(s,I||hash(R))||R,** as the digital ticket; wherein the reading into the computer of the ticket taker is of the **Sign(s,I||hash(R))||R;** wherein the recovering in the computer of the ticket taker of the **I||hash (R)** gives **hash (R)**; and, having both **R and hash (R)** to hand" is met on column 11, lines 14-67 and on column 12, lines 1-15. Further limitation of "wherein the determining further proceeds by recalculating the **hash(R)** in respect of R, so that IF the recalculated **hash(R)** equals

to the recovered **hash(R)** of the digital ticket as read THEN the digital ticket is valid ELSE IF the **hash(R)** does not equal to the recovered **hash(R)** of the digital ticket as read THEN the digital ticket is invalid" is met inherently on column 12, lines 7-9.

With respect to Claim 5, the limitation of "wherein the determining still further proceeds so that IF the read digital ticket is the first uniquely presented THEN the digital ticket is valid ELSE IF the read digital ticket is not the first uniquely presented THEN the digital ticket is invalid" is met on column 25, lines 15-18.

With respect to Claim 8, the limitation of "first transmitting, across a communications channel from a computer of a ticket provider to a computer of a prospective ticket consumer, data regarding an event for which tickets may be delivered; and then, the prospective ticket consumer deciding to obtain a ticket for a particular selected event and thus to become a ticket consumer" is met on column 4, lines 33-39, 45-50; and "first calculating in the computer of the ticket consumer a number R; then second calculating in the computer of the ticket consumer a one-way function of the number **R as hash(R)"** is met on column 12, lines 1-15; and "second transmitting, across the communications channel from the computer of the ticket consumer to the computer of the ticket ticket request being capable of being fulfilled third calculating in the computer of the ticket provider in respect of signature key s a digital signature of **hash(R)** appended to information I regarding the event as **Sign(s,I||hash(R))** , this **Sign(s,I||hash(R))** constituting a digital ticket precursor; then third transmitting, across the communications channel from the computer of the ticket provider to the computer of the ticket consumer,

the digital ticket precursor **Sign(s,I||hash(R));** fourth calculating, in the computer of the ticket consumer as an appending of R to the digital ticket precursor Si**gn(s,I||hash(R)), Sign(s,I||hash(R))||R,** as a digital ticket;" is met on column 11, lines 14-67 and column 12, lines 1-15; and "first storing the digital ticket **Sign(s,I||hash(R))** I IR from the computer of the ticket consumer to a transportable storage medium" is met on column 25, lines 64-67 and on column 26, lines 1-3.

It would have been obvious to one of ordinary skill in the art to have X represent a random number R because X is a function of a hash, which is inherently a random number generator. Hence X will always yield a unique value.

With respect to Claim 9, the limitation "transporting the transportable storage medium within which the digital ticket **Sign(s,I||hash(R))||R** is written to the particular selected event," is met on column 26, lines 25-40 and on column 4, lines 41-44; and "tendering the digital ticket within the transportable storage medium for verification and for admission to the particular selected event" is met on column 25, lines 3-6; and "reading the digital ticket **Sign(s,I||hash(R))||R** to an event computer" is inherently met on column 25, lines 24-26; and "extracting in the event computer the number R from the read **Sign(s,I||hash(R))||R"** is met on column 19, lines 8-12; and "fifth calculating, by use of a verification key V complimentary to the signature key **s, I||hash(R);"** is met on column 19, lines 13-31; and **"**sixth calculating in the event computer, with the same one-way function previously used in the second calculating, **hash(R)**; and then, having both R and sixth-calculated **hash(R)** to hand, comparing the sixth- calculated **hash(R)** to the **hash(R)** portion of the fifth-calculated **I11hash(R)"** is met on column 12, lines 1-

15. Further limitation of "wherein IF the fifth-calculating proceeds correctly AND the information I is correct for the event AND the sixth- calculated **hash(R)** compares to the fifth- calculated **hash(R)** of the digital ticket as read **THEN** grant admission to a holder of the digital ticket ELSE IF the fifth-calculating proceeds incorrectly OR the information I is incorrect for the event OR the sixth- calculated **hash(R)** fails to compares to the fifth-calculated **hash(R)** of the digital ticket" is met on column 12, lines 7-9 and in Fig. 23B.

With respect to Claim 10, the limitation "wherein IF the fifth-calculating proceeds correctly AND the information I is correct for the event AND the sixth- calculated **hash(R)** compares to the fifth calculated **hash(R)** s the first uniquely presented **THEN** grant admission to a holder of the digital ticket **ELSE IF** the fifth-calculating proceeds incorrectly OR the information I is incorrect for the event OR the sixth- calculated **hash(R)** fails to compares to the fifth-calculated **hash(R)** of the digital ticket as read OR the read digital ticket is not the first uniquely presented **THEN** deny admission to the holder of the digital ticket" is met on column 12, lines 1-15 and in Fig. 23B.

With respect to Claim 11, the limitation "second storing R in the event computer as an indication that the digital ticket has been tendered" is met on column 9, lines 23-32 and on column 25, lines 36-42.

With respect to Claim 12, the limitation "where the ticket provider is also a ticket seller, the ticket consumer is also a ticket buyer, and the delivery of the ticket to the ticket

consumer across the communications channel accompanies a sale of the ticket wherein the second transmitting further includes electronic payment suitable to the order data" is met on column 3, lines 66-67 and on column 4, lines 1-39.

With respect to Claim 13, the limitation "wherein the first transmitting, the second transmitting and the third transmitting are upon a worldwide communications network" is met on column 2, lines 4-8.

With respect to Claim 14, the limitation "wherein the first transmitting, the second transmitting and the third transmitting are upon a worldwide secure or encrypted communications network" is met on column 2, lines 9-11.

With respect to Claim 15, the limitation "wherein the first transmitting, the second transmitting and the third transmitting are upon the Internet" is met on column 2, lines 4-8.

With respect to Claim 17, the limitation "wherein the first storing is in a transportable medium subsequently physically deliverable to the site of the particular selected event to there be tendered as a digital ticket by the ticket consumer" is met on column 25, lines 64-67 and on column 26, lines 1-3.

With respect to Claim 22, the limitation "wherein the first storing in the transportable medium of a computer disk" is met on column 25, lines 64-67 and on column 26, lines 1-3.

With respect to Claim 24, the limitation "a ticket consumer's computer, connected to the communications network" is met on column 2, lines 4-8; and "for first transmitting ticket order data upon the communications network to a ticket provider's computer" is met in Fig. 23A; and "for first receiving upon the communications network from the ticket provider's computer a digitally signed ticket data" in Fig. 23A and on column 6, lines 7-12, and "for storing the digitally signed ticket data in a transportable storage medium" on column 25, lines 64-67 and column 26, lines 1-3; and "a ticket provider's computer, connected to the communications network" on column 2, lines 4-8; and "for second receiving from the ticket consumer's computer upon the communications network the first -transmitted ticket order data" in Fig. 23A; and "for digitally signing the ticket data" on column 6, lines 7-12 and column 12, lines 1-3; and "and for second transmitting the digitally signed ticket data upon the communications network to the ticket consumer's computer and a communications network, for communicating at a first time the first – transmitting of the ticket consumer's computer to the second-receiving of the ticket provider's computer, and for communicating at a second time the fourth-transmitting of the ticket provider's computer to the first-receiving of the ticket consumer's computer" in Fig. 23A.

With respect to Claim 25, the limitation "wherein the ticket consumer's computer is first calculating a number R, and is second calculating a one way function of R to produce **hash(R)** as ticket data" is met on column 12, lines 1-15; and "wherein the first transmitting is of the second-calculated **hash(R)** as the ticket data, wherein the first receiving is) of **hash(R)** and additional information I digitally signed with signature key S as **Sign(s,I||hash(R)),** is third calculating an appending of R to the digital ticket precursor **Sign(s,I||Ihash(R)),** giving **Sign(s,I||hash(R))||R** as a digital ticket, and wherein the storing is of the third-calculated digital ticket **Sign(s,I||hash(R))||R;** wherein the ticket provider's computer is second receiving the first -transmitted **hash(R)** ticket order data, is calculating a digital signature in respectof the ticket data, and additional information I, in respect of signature key **s as Sign(s,I||hash(R)),** and is second transmitting the calculated **Sign (s, I||hash (R)"** is met on column 11, lines 14-67 and on column 12, lines 1-15.

With respect to Claim 29, the limitation "for first calculating a number R" is met on column 12, lines 1-15; and "for second calculating a one way function of R to produce **hash(R)** as ticket data" is met on column 12, lines 1-15; and "for first transmitting the second calculated **hash(R)** ticket data upon the communications network to a ticket provider's computer as a ticket data for a particular selected event for first receiving upon the communications network a digitally signed data in respect of signature key **s of hash(R)** and additional information **I as Sign(s,I||hash(R)),** for third calculating an appending of R to the digital ticket precursor **Sign(s,I||hash(R))** so as to give **Sign(s,I||hash(R))||R** as a digital ticket" on column 11, lines 14-67 and on column 12,

lines 1-15; and "for first storing the third- calculated digital ticket **Sign(s,I||hash(R))||R** in a transportable storage medium" on column 25, lines 64-67 and on column 26, lines 1-3; and "a ticket provider's computer, connected to the communications Network" on column 2, lines 4-8; and "for second receiving from the ticket consumer's computer upon the communications network the first -transmitted **hash(R)** ticket data, for fourth calculating digitally signed data in respect of signature key s of second-received **hash(R)** and of information **I as Sign(s,I||hash(R)),** and for second transmitting the fourth-calculated **Sign(s,I||hash(R))** upon the communications network to the ticket consumer's computer; and a communications network" on column 11, lines 14-67 and on column 12, lines 1-15; and "for communicating at a first time the first –transmitting of the ticket consumer's computer to the second-receiving of the ticket provider's computer, and for communicating at a second time the fourth- transmitting of the ticket provider's computer to the first-receiving of the ticket consumer's computer" in Fig. 23A.

With respect to Claim 30, the limitation of "a tangible transportable data storage medium containing a digital signature of an issuer of the ticket" is met on column 25, lines 64-67 and on column 26, lines 1-3 and "wherein the tangible transportable data storage medium contains **Sign (s, I hash (R)**||R where R is a random number private to the ticket consumer, **hash(R)** is a one-way function of R, and **Sign(s,I||hash(R))** is a digital signature, in respect of signature key s private to the ticket provider, of the **hash(R)** appended to information I" is met on column 25, lines 64-67, column 26, lines 1-3, column 11, lines 14-67 and on column 12, lines 1-15.

With respect to Claim 32, its limitation is contained within Claim 30 limitation and hence its rejection can be found therein.

With respect to Claim 33, the limitation "a tangible transportable data storage medium containing **Sign(s,I||hash(R))||R"** is met on column 25, lines 64-67 and on column 26, lines 1-3; and where (1) R is a number having its origin in a computer of the ticket consumer, which number R is appended to (2) a number **Sign(s,I||hash(R))** that was computed in a computer of the ticket provider as a digitally signature signed data in respect of a signature key s of a number **hash(R)** appended to information I, thus **Sign(s,I||hash(R)),** and subsequently communicated across the communications network to the computer of the ticket consumer, which number **hash(R)** was itself computed in the computer of the ticket provider consumer as a one way function of R, thus **hash(R),** and subsequently communicated to the computer of the ticket provider; wherein number R, having its origin in a computer of the ticket consumer, is private to the ticket consumer and is not public" is met on column 11, lines 14-67 and on column 12, lines 1-15; and "wherein the digital signature key s of the computer of the ticket provider is private to the ticket provider and is not public" is met on column 7, lines 30-38.

With respect to Claim 34, the limitation "a tangible transportable digital data storage medium containing" is met on column 25, lines 64-67 and on column 26, lines 1-3; and "first-type data, originally known both to a buyer and to a seller of a ticket and meaningful to at least the seller of the particular event for which the ticket was sold" is

met by Fig. 2, ref. nos. 88; and "second-type data including a signed digital representation of a particular parameter that was originally computer-generated in sequence" is met on column 7, lines 30-32; and "first by the buyer of the ticket as a non-invertible function of a random number called a "first-time-made non-invertible function" and second by the seller of the ticket as a digital signature of the first-time-made non-invertible function" on column 11, lines 30-67 and on column 12, lines 1-15. The non-invertible function is represented by the hash(X). X represents the random number. Further limitation of "third by the buyer of the ticket to attach the selfsame random number" on column 19, lines 6-12; and "wherein, to validate the digital ticket upon attempted redemption of the ticket" on column 19, lines 13-31; and "the random number is detached, and then the signed first-time-made non-invertible function is interpreted, recovering this first-time-made non-invertible function" on column 19, lines 6-12; and "the non-invertible function of that selfsame random number just detached is newly made all over again, which newly made non-invertible function is called the second-time-made non-invertible function " on column 19, lines 50-61 ; and "wherein the second- time -made non-invertible function EITHER equals the first-time-made ,non-invertible function in which case the ticket is not invalid OR ELSE the second-time-made non-invertible function does not equal the first-time-made non-invertible functional thus making the digital ticket is invalid for at least the particular event" is met on column 24, lines 41-64.

With respect to Claim 35, the limitation "wherein the digital signature within the tangible medium as read by a digital reader is further compared to a data base of digital

tickets actually signed and sold not so as to determine whether a tendered digital ticket is valid or invalid but rather for statistical purposes" is met on column 7, lines 56-61.

With respect to Claim 49, the limitation "a ticket buyer computer (i) sending at a first time a one-way transformation of a private number to a seller computer, (ii) receiving at a third time signed information from the ticket seller computer, and (iii) storing at a fourth time within a digital store the received encrypted signed information plus the private number" is met on column 12, lines 1-15 and column 9, lines 24-32. Further limitation of "a ticket seller computer (i) receiving at the first time the one-way transformation of the private number from the seller computer, (ii) signing at a second time this one-way transformation and additional information, and (iii) sending at the third time the signed first trans format. ion and additional information to the ticket buyer computer as signed information" is met by Fig. 23A and on column 12, lines 1-15; and "a digital store storing at the fourth time the signed information plus the private number as a digital ticket" is met on column 25, lines 66-67 and on column 26, lines 1-3; and "wherein upon (i) a reading of the signed information, (ii) a decrypting of the signed information to recover the one-way transformation of the private number, (iii) a reproducing with the same secure first transformation that the ticket seller used the secure first transformation of the number all over again, and (iv) a comparing of the decrypted recovered one-way transformation to the reproduced first trans formation, validity of the digital ticket is assessable" is met on column 12, lines 1-15, and column 24, lines 49-61.

With respect to Claim 50, the limitation "first-sending at a first time a one-way transformation of a private number from a ticket buyer computer to a ticket seller computer first-receiving at the first time the one-way transformation of the private number in the ticket seller computer" is met on column 11, lines 14-67 and on column 12, lines 1-15; and "signing at a second time the one-way transformation and additional information in the ticket seller computer" is met on column 11, lines 14-67; and "second-sending at a third time the signed first transformation and additional information as signed information from the ticket seller computer to the ticket buyer computer" is met on column 11, lines 14-67 and on column 12, lines 1-15; and "second-receiving at the third time the signed information in the ticket buyer computer" is met on column 12, lines 1-15; and "storing with the ticket. buyer computer at a fourth time both (i) the received signed information plus (ii) the private number within a digital memory store" is met on column 9, lines 23-32; and "storing within the digital memory store at the fourth time the signed information plus the private number as a digital ticket" is met on column 25, lines 66-67 and on column 26, lines 1-3; and "wherein upon (i) a reading of the signed information, (ii) a decrypting of the signed information to recover the one-way transformation of the private number, (iii) a reproducing, with the 45 same secure first transformation that the ticket seller used, the secure first transformation of the number all over again, and (iii) a comparing of the decrypted recovered one-way transformationto the reproduced first transformation, validity of the digital ticket is assessable" is met on column 24, lines 49-61.

Claims 6, 7, 16, 18-21, 23, 26-28, 36, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosen (5557518) in view of Mengin et al (US2002/0095383 A1).

With respect to Claim 6, all the limitation is met by Rosen except the limitation disclosed below.

The limitation of "wherein the calculating is of digital signature suitably displayed as a 2-D code" is met by Mengin et al on paragraph 31, 59; and "wherein the first storing with the computer of the ticket consumer is by printing of the 2 –D code upon a printable transportable storage medium" is met by Mengin et al on paragraph 17.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because a digital signature is a well known method of authentication and hence the ticket can be authenticated when it is presented for use by the user.

With respect to Claim 7, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the reading into a computer of the ticket taker of the digital signature transpires by use of an optical reader" is met by Mengin et al on paragraph 31.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen

because a digital signature is a well known method of authentication and hence the ticket can be authenticated when it is presented for use by the user.

With respect to Claim 16, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the first transmitting, the second transmitting and the third transmitting are upon the Secure Socket Layer (or SSL) of the Internet" is met by Mengin et al on paragraph 39.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because SSL is a well known method of encryption and hence preventing an attacker from deciphering the transmitted information.

With respect to Claim 18, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the first storing is in the transportable medium of a printed substrate" is met by Mengin et al on paragraph 79; and "wherein the printed encrypted digital record is subsequently physically deliverable to the site of the particular selected event

to there be tendered as the digital ticket by the ticket consumer" on paragraph 40 and 62 of Mengin et al.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen

because a printed substrate is a portable and convenient form for the user to manifest the ticket. It is very common and convenient method to have an electronic ticket print out on a substrate at the user's terminal.

With respect to Claim 19, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the first storing in the transportable medium of a printed substrate is in form of a two-dimensional bar code" is met by Mengin et al on paragraphs 31, 59 and 17.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because a printed substrate is a portable and convenient form for the user to manifest the ticket. It is very common and convenient method to have an electronic ticket print out on a substrate at the user's terminal

With respect to Claim 20, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "printed two-dimensional bar code is in accordance with the PDF417 standard" is met by Mengin et al on paragraphs 31, 59 and 17.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because this is a given printing standard at most computers.

With respect to Claim 21, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the first storing in the transportable medium of a printed two-dimensional bar code is in accordance with the QR standard." is met by Mengin et al on

paragraphs 31, 59 and 17.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because this is a given printing standard at most computers.

With respect to Claim 23, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the first storing is in the transportable medium of a smart card; wherein the digital record stored within the smart card is subsequently physically deliverable

to the site of the particular selected event to there be tendered as the digital ticket by the ticket consumer" is met by Mengin et al on paragraphs 19 and 20.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because a smart card provides a more secure way of storing the ticket.

With respect to Claim 26, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the ticket consumer's computer is storing the digital ticket by printing it" is met by Mengin et al on paragraph 17.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because printing the ticket at the user's terminal is a common way of manifestation of an electronic ticket.

With respect to Claim 27, 28, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the ticket consumer's computer is storing the digital ticket by printing it in a 2-D machine-readable (bar-code) pattern" is met by Mengin et al on paragraph 17.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because a bar code ensures uniqueness of each ticket provided to each individual user. Hence authentication is easier to execute.

With respect to Claim 36, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the digital signature within the tangible medium is visible to the eye" is met by Mengin et al on paragraph 31.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen

because it would be a quicker form of authentication for the service provider to be able to eyeball the digital signature and know immediately if the ticket is valid or not.

With respect to Claim 37, all the limitation is met by Rosen except the limitation disclosed below.

The limitation "wherein the digital signature visible to the eye is comparable by eye to a catalog of visual sensible representations of digital tickets actually signed and sold in order to determine whether a tendered digital ticket is valid or invalid" is met by Mengin et al on paragraph 33.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Mengin et al within the system of Rosen because it would be a quicker form of authentication for the service provider to be able to eyeball the digital signature and know immediately if the ticket is valid or not.

Claim 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mengin et al (US2002/0095383 A1) in view of Rosen (5557518).

With respect to Claim 48, all the limitation is met by Mengin et al except the limitation disclosed below.

The limitation of "the 2-D bar coded indicia contains Sign(s,I||hash(R))||R where (1) R

is a number having its origin in a computer of a consumer of the ticket, which number R is appended to (2) a number Sign(s,I||hash(R)) that was computed in a computer of a

provider of the ticket as a digital signature in respect of digital signature key s of the number hash(R) in combination with information I, subsequently communicated across the communications network to the computer of the ticket consumer, which number hash(R) was itself computed in the computer of the ticket provider as a one way function of R and subsequently communicated to the computer of the ticket provider; wherein number R, having its origin in a computer of the public; and wherein the digital signature key s of the computer of the ticket provider is private to the ticket provider and is not public" is met by Rosen on column 11, lines 14-67 and on column 12, lines 1-15.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Rosen within the system of Mengin et al because having a signature containing a hash function of a number within the bar code makes it unique since the hash function is a one to one function. Therefore, the bar code will be unique for each ticket it appears on.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 38-46 and 51-55 are rejected under 35 U.S.C. 102(e) as being anticipated by Mengin et al (US2002/0095383 A1).

With respect to Claim 38, the limitation "a communication channel for at a first time sending from a ticket seller to a ticket buyer data regarding events for which tickets may be had" is met on paragraphs 11, 14 and 29; and "at a second time sending from the ticket buyer to the ticket seller data representative of a non-invertible transformation of a number determined by the ticket buyer only" is met on paragraph 53; and "at a third time sending from the ticket seller to the ticket buyer a digital signature of the non-invertible transformation" on paragraph 55; and "a ticket buyer's computer, communicatively connected to the communications channel, for (i) determining the number, (ii) computing the non-invertible trans format ion, and (iii) combining the non-invertible transformation with the number to produce a digital ticket" is met on paragraphs 54 and 55; and "a ticket seller's computer, communicatively connected to the communications channel, f or computing, in respect of the non-invertible transformation received from the buyer, the digital signature of the non-invertible transformation" is met on paragraph 46 and 56 and "a tangible portable medium of digital data storage connected to the buyer's computer for storing the digital ticket, and for transporting this digital ticket to a physical site of the particular selected event, where it may be used for admission" is met on paragraph 63.

With respect to Claim 39, the limitation "wherein the communication channel is sending at the second time a random number" is met on paragraph 20.

With respect to Claim 40, the limitation "wherein the communication channel is sending at the second time a number representing the particular selected event" is met on paragraph 29.

With respect to Claim 41, the limitation "a worldwide digital communications network" is met by paragraph 48.

With respect to Claim 42, the limitation "wherein the communication channel comprises: a worldwide secure digital communications network" is met on paragraph 48 and 39.

With respect to Claim 43, the limitation "wherein the tangible portable medium of digital data storage comprising a computer disk" is met on Fig. 4.

With respect to Claim 44, the limitation "wherein the tangible portable medium of digital data storage comprises a printed medium" is met on paragraph 79.

With respect to Claim 45, the limitation "indicia includes a 2-D bar code containing absolutely all necessary information by which the legitimacy, if not the uniqueness, of the ticket may be determined" is met on paragraph 31; and "the 2-D bar coded indicia contains a one-way function of a number provided by a holder of the ticket" is met on paragraph 53-55.

With respect to Claim 46, the limitation "the 2-D bar coded indicia contains data digitally signed by the provider of the ticket" is met on paragraph 31.

With respect to Claim 51, the limitation of "at a first time first-sending from the computer of the ticket seller across the communications network to the computer of the ticket buyer first data regarding events for which tickets may be had" is met on paragraphs 11,14, 29; and "then at a second time second-sending from the computer of the ticket buyer across the communications network to the computer of the ticket seller second data identifying an event for which a ticket is desired, the second data accompanied by a secure first transformation of a number that is determined by the ticket buyer only and unknown to others including the ticket seller; then at a third time" is met on paragraph 53; and "third-sending from the computer of the ticket seller across the communications network to the computer of the ticket buyer third data confirming ticketing to the event for which the ticket was desired, the third data accompanied by a secure second transformation of the secure first transformation" is met on paragraph 55; and "storing, with the (computer of the ticket buyer within a tangible portable medium of digital data storage, (i) the number in accompaniment to (ii) the secure second transformation" is met on Fig. 4; and "wherein upon (i) transportation. of the digital data storage medium to a physical site of the event, (ii) reading of the number to a computer, and, by use of the same secure first transformation that the buyer did use, reproduction of the secure first transformation of the number all over again, plus (iii) reversing of the secure second transformation by an event computer privileged to knowledge of said second transformation, then a (ii) read and reproduced first transformation is comparable to a (iii) first transformation recovered

from reversing the second transformation in order to assess validity of the digital ticket" is met on paragraphs 62, 63 and 82.

With respect to Claim 52, the limitation "wherein the second-sending is of the second data accompanied by a secure first transformation in the form of a one-way hash function of the number" is met on paragraph 53.

With respect to Claim 53, the limitation "wherein the third-sending is of the second data accompanied by a secure transformation in the form of a digital signature of the secure first transformation" is met on paragraph 55.

With respect to Claim 54, the limitation "wherein the storing within a tangible portable medium of digital data storage comprises printing" is met on paragraph 79.

With respect to Claim 55, the limitation "wherein the printing is of at least the (ii) secure second transformation in the form of a two-dimensional bar code" is met on paragraph 31.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 571-272-3846. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OTA